Toward Ogg's Conjecture for $J_0(N)$

Kenneth A. Ribet

May 10, 2022

Dedicated to Bas Edixhoven

Thesis defense, 1989

Joint work with Preston Wake

December, 2019

Setup

$N \geq 1$, $Y_0(N) \hookrightarrow X_0(N) = Y_0(N) \coprod \{\text{ cusps }\}$, all over $\mathbf{Q}$.

$J_0(N) =$ Jacobian of $X_0(N)$ (Abelian variety over $\mathbf{Q}$).

$\tilde{C} =$ group of degree-0 divisors on $X_0(N)$ with cuspidal support (formal cuspidal group)

$C =$ image of $\tilde{C}$ in $J_0(N) =$ cuspidal subgroup of $J_0(N)$.

Manin–Drinfeld: C is a finite group

Note: C consists of *rational* torsion points of $J_0(N)$ if N is square free (but not in general).

Example: the case where N is prime

If N is prime, then C is the cyclic subgroup generated by the image of $(\infty) - (0)$ in $J_0(N)$. It has order $n = \text{num}\left(\frac{N-1}{12}\right)$.

Theorem (Mazur, 1977)

The group C is the full group of rational torsion points of $J_0(N)$.

For example, C has order 5 if $N = 11$, order 11 if $N = 23$, etc., etc.

Mazur's theorem was *Ogg's conjecture* before it was proved in the *Eisenstein ideal* article by Mazur.

Inventiones math. 12, 105–111 (1971)

Rational Points of Finite Order on Elliptic Curves

A. P. OGG* (Berkeley, California)

If A is an abelian curve defined over the field of rational numbers $\mathbf{Q}$, then by Mordell's theorem the group $A_{\mathbf{Q}}$ of rational points on A is of finite type:

$$A_{\mathbf{Q}} \simeq \mathbf{Z}^r \oplus F,$$

where F is finite. According to Cassels [2, p.264], the folklore contains the conjecture that the order of F is bounded, and in particular there should be only a finite number of integers N such that some curve A has a rational point of order N. It is known [2, p.264] that $N=1-10$ or 12 is possible, and that $N=11$, 14, 15, 16, 20, or 24 is impossible.

In the present paper, we give a proof that $N=17$ is impossible, by a suitable modification of the method used by Billing and Mahler [1] to prove that $N=11$ is impossible, and then make some general remarks on the modular interpretation of the problem.

The general Ogg conjecture

William Stein filed his PhD thesis in 2000 and began computing with modular symbols, modular forms, modular curves,... even while a graduate student. Stein's work (especially Sage) made it practical to compute C for N not too big (say less than 1000) and to have some confidence in the following conjecture.

Conjecture (Ogg's conjecture for $N \geq 1$)

If N is a positive integer, the group of rational torsion points of $J_0(N)$ is contained in C.

A related problem

Can one give a neat (conjectural) characterization of C inside the group of all torsion points of $J_0(N)$?

Literature on Ogg's conjecture

In 2013 and 2014, Masami Ohta proved Ogg's conjecture for N square free away from the 2- and 3-primary parts of the finite abelian groups C and $J_0(N)(\mathbf{Q})_{\text{tors}}$. In addition, he treats the 3-primary parts if N is not divisible by 3. To do this, he finds the order of $J_0(N)(\mathbf{Q})_{\text{tors}}$ and compares the result with Takagi's 1997 computation of the order of C.

Other authors who have worked on aspects of the problem include D. Lorenzini, Conrad–Edixhoven–Stein, H. Yoo and Y. Ren.

Our perspective

The aim is to prove Ogg's conjecture by a "pure thought" that avoids computing the orders of the groups being compared.

We succeed at least when N is square free and for p-primary parts if p is at least 5 and prime to N.

A convention

From now on, fix $N \geq 1$ and a prime p not dividing $6N$.

We localize abelian groups systematically at the ideal (p) of $\mathbf{Z}$ but commit the serious abuse of notation by writing simply "A" instead of "$A_{(p)}$" when A is an abelian group.

Our first theorem

To state said theorem, we need a bunch of notation. Let M be the space of weight-2 holomorphic modular forms on $\Gamma_0(N)$ and let $S \subseteq M$ be the space of cusp forms. Let $E \subseteq M$ be the complementary space of Eisenstein series. On all three spaces M, S and E, we have the classical Hecke operators T_n for $n \geq 1$. (Note to experts: we use T_q instead of w_q for q a prime dividing N.) Consider the Hecke ring

$$\tilde{\mathbf{T}} = \mathbf{Z}[\ldots, T_n, \ldots] \subseteq \operatorname{End} M$$

along with the corresponding rings

$$\mathbf{T} = \mathbf{Z}[\ldots, T_n, \ldots] \subseteq \operatorname{End} S, \quad \mathbf{T}_E = \mathbf{Z}[\ldots, T_n, \ldots] \subseteq \operatorname{End} E$$

for S and E.

The asymmetry in the notation ($\mathbf{T}$ instead of $\mathbf{T}_S$) reflects our perspective that $\tilde{\mathbf{T}}$ and its quotient $\mathbf{T}$ are the objects of primary interest, while $\mathbf{T}_E$ is of secondary importance.

Our first theorem

The *Eisenstein ideal* of $\tilde{\mathbf{T}}$ is the kernel of the quotient map $\tilde{\mathbf{T}} \to \mathbf{T}$ defined by restriction to S. The *Eisenstein ideal* of $\mathbf{T}$ is the image in $\mathbf{T}$ of the Eisenstein ideal of $\tilde{\mathbf{T}}$.

For each prime q not dividing N, the operator $1 + q - T_q$ of $\tilde{\mathbf{T}}$ annihilates E and thus belongs to the Eisenstein ideal of $\tilde{\mathbf{T}}$.

Theorem

If Σ is a finite set of prime numbers containing the primes dividing N, then the Eisenstein ideal of $\tilde{\mathbf{T}}$ is generated by the $1 + q - T_q$ with q not in Σ.

Reminder: we are localizing away from $6N$.

The Eisenstein ideal of $\mathbf{T}$

Let $I \subseteq \mathbf{T}$ be the Eisenstein ideal (the image in $\mathbf{T}$ of the Eisenstein ideal of $\tilde{\mathbf{T}}$).

Corollary

If Σ is a finite set of prime numbers containing the primes dividing N, then the Eisenstein ideal I is generated by the $1 + q - T_q \in \mathbf{T}$ with q not in Σ.

Application: rational torsion points are Eisenstein

The Eichler–Shimura formula shows that the finite group $J_0(N)(\mathbf{Q})_{\mathrm{tors}}$ is annihilated by the operators $1 + q - T_q$ in $\mathbf{T}$ for all q prime to N and the order of $J_0(N)(\mathbf{Q})_{\mathrm{tors}}$. Hence we obtain the following consequence:

Corollary

The group $J_0(N)(\mathbf{Q})_{\mathrm{tors}}$ is annihilated by the Eisenstein ideal of $\mathbf{T}$. In symbols, $I \subseteq \operatorname{Ann}_{\mathbf{T}} J_0(N)(\mathbf{Q})_{\mathrm{tors}}$.

Our second theorem

Recall that C is the cuspidal subgroup of $J_0(N)$. Our second theorem is a quantitative "small annihilator" version of the qualitative statement that C is "big."

Theorem

The annihilator of C in $\mathbf{T}$ is contained in the Eisenstein ideal I.

Ogg's conjecture

Theorem

The annihilator of C in $\mathbf{T}$ is contained in the Eisenstein ideal I.

Corollary (of the first theorem)

The group $J_0(N)(\mathbf{Q})_{\mathrm{tors}}$ is annihilated by the Eisenstein ideal of $\mathbf{T}$. In symbols, $I \subseteq \mathrm{Ann}_{\mathbf{T}}\, J_0(N)(\mathbf{Q})_{\mathrm{tors}}$.

These two statements combine to prove that the annihilators of C and $J_0(N)(\mathbf{Q})_{\mathrm{tors}}$ are *equal*. Ogg's conjecture follows directly from this equality plus the following cyclicity result à la Mazur.

Proposition

For each maximal ideal $\mathfrak{m}$ of $\mathbf{T}$, the kernel $J_0(N)(\mathbf{Q})_{\mathrm{tors}}[\mathfrak{m}]$ is a cyclic $\mathbf{T}/\mathfrak{m}$-vector space.

Ogg's conjecture

By Nakayama's lemma, the cyclicity in the proposition shows that the Pontryagin dual of $J_0(N)(\mathbf{Q})_{\text{tors}}$ is a cyclic $\mathbf{T}$-module. An evident quotient is the Pontraygin dual of C. Since the module and its quotient are cyclic and have identical annihilators, they are equal.

Discussion of the first theorem

The first theorem concerns the Eisenstein ideal of $\tilde{\mathbf{T}}$, which is the kernel of the restriction map $\tilde{\mathbf{T}} \to \operatorname{End} E$. The image of this map is the Eisenstein Hecke ring, whose $\mathbf{Z}$-rank is $2^r - 1$, where r is the number of primes dividing N.

The Eisenstein ideal of $\tilde{\mathbf{T}}$ contains these elements:

- $1 + q - T_q$ for *all* primes q prime to N,
- $(T_q - 1)(T_q - q)$ for all primes q dividing N,
- the product $\prod_q (T_q - 1)$, taken over all q dividing N.

Taken together, these elements generate the Eisenstein ideal: the quotient of the formal polynomial ring $\mathbf{Z}[\ldots, T_n, \ldots]$ by the elements is a free $\mathbf{Z}$-module of the same rank as $\mathbf{T}_E$.

To prove the theorem is to show that these “bulleted” elements all lie in the ideal generated by the $1 + q - T_q$ with q outside Σ.

Some notation

Let $\tilde{I} \subseteq \tilde{\mathbf{T}}$ be the Eisenstein ideal of $\tilde{\mathbf{T}}$ and let $\tilde{J} \subseteq \tilde{I}$ be the ideal generated by the $1 + q - T_q$ with q not in Σ. Then $\tilde{J} \subseteq \tilde{I}$. The theorem states the opposite inclusion, to the effect that the bulleted elements all lie in $\tilde{J}$.

We prove that these elements lie in $\tilde{J}$ by studying Galois representations.

To show $\tilde{I} \subseteq \tilde{J}$, it's convenient to work locally, "prime" (i.e., maximal ideal $\mathfrak{m} \subset \tilde{T}$) by prime. We can assume that $\tilde{J} \subseteq \mathfrak{m}$; otherwise, there is nothing to prove. This assumption means that $\mathfrak{m}$ contains almost all of the $1 + q - T_q$, which is the same as saying that the mod p representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ associated to $\mathfrak{m}$ is a reducible representation.

The Hecke ring (revisited)

The Hecke ring $\tilde{\mathbf{T}}$ is (by definition) a $\mathbf{Z}_{(p)}$-algebra. The associated $\mathbf{Q}$-algebra $\tilde{\mathbf{T}} \otimes \mathbf{Q}$ is a product of number fields because of a result of Coleman–Edixhoven ("On the semi-simplicity of the U_p-operator on modular forms").

To get p-adic Galois representations, we consider for a moment the p-adic completion $\tilde{\mathbf{T}} \otimes \mathbf{Z}_p$, which is a semi-local ring: a product of local rings $\prod_{\mathfrak{m}} \mathbf{T}_{\mathfrak{m}}$, with the factors indexed by the maximal ideals of $\tilde{\mathbf{T}}$. Each $\mathbf{T}_{\mathfrak{m}}$ is an order in a product of p-adic integer rings; the $\mathbf{Q}_p$-algebra $\mathbf{T}_{\mathfrak{m}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is then a product of p-adic fields.

The Hecke ring (revisited)

Without losing information, we can and will now replace $\tilde{\mathbf{T}}$ by its p-adic completion $\tilde{\mathbf{T}} \otimes \mathbf{Z}_p$. In fact, let's go further and fix a maximal ideal $\mathfrak{m}$ as "above" and replace $\tilde{\mathbf{T}}$ by $\mathbf{T}_m$.

We can and will assume that $\tilde{J} \subseteq \mathfrak{m}$, and we write simply $\tilde{J}$ for the ideal $\tilde{J}_{\mathfrak{m}}$ that $\tilde{J}$ generates in $\tilde{\mathbf{T}}_{\mathfrak{m}}$.

Galois representations

There is a natural Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, \tilde{\mathbf{T}})$$

with determinant equal to the p-adic cyclotomic character $\chi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_p^*$ for which

$$\mathrm{trace}(\rho(\mathrm{Frob}_q)) = T_q \in \tilde{\mathbf{T}}$$

for almost all q. By Čebotarev, trace(ρ) takes values in $\tilde{\mathbf{T}}$; and $\tilde{J} \subseteq \tilde{\mathbf{T}}$ is the ideal generated by the image of the function

$$\mathrm{trace}(\rho) - \chi - 1 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \tilde{\mathbf{T}}.$$

Using this characterization of $\tilde{J}$, we show that $\tilde{J}$ contains all of the bulleted relations.

Example: N=11

In the case $N = 11$ that was considered by Mazur in 1977, the ring $\tilde{\mathbf{T}}$ (before localization) is the order of index 5 in $\mathbf{Z} \times \mathbf{Z}$, with (say) the second factor corresponding to the 1-dimensional space of Eisenstein series and the first factor corresponding to the elliptic curve $J_0(11)$. Take $p = 5$. After p-adic completion, the ring $\tilde{\mathbf{T}}$ is $\{\, (a, b) \in \mathbf{Z}_p \mid a \equiv b \pmod{5} \,\}$. It has a single maximal ideal. The tensor product $\tilde{\mathbf{T}} \otimes \mathbf{Q}_p$ is a product of two copies of $\mathbf{Q}_p$. The Galois representation that we have just introduced is the direct sum of the irreducible 2-dimensional representation arising from $V_5(J_0(11))$ and the 2-dimensional representation $1 \oplus \chi$.

Example of a bulleted relation

Drew and Rachel suggested that I make my slides available to people who attend my talk. I'm including a the next slide for offline reading with the idea that I'll never have time to discuss it during my "live" talk.

Example of a bulleted relation

One of the bulleted relations is $(T_q - 1)(T_q - q)$ for q a prime dividing N. Take such a q, and note that q and p are distinct. Let $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be a Frobenius element for q: one chooses first a decomposition group for q in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and then an element of the decomposition group that maps to the usual Frobenius element in the unramified quotient of the decomposition group.

One checks, component by component, that

$$T_q^2 - \mathrm{trace}\,\rho(\mathrm{Frob}_q)\,T_q + q = 0.$$

The representation ρ could well be ramified at q, but the semisimplification of its restriction to the decomposition group is unramified. Modulo $\tilde{J}$, $\mathrm{trace}\,\rho(\mathrm{Frob}_q) \equiv 1 + \chi(\mathrm{Frob}_q) = 1 + q$, so that

$$T_q^2 - (1+q)T_q + q \in \tilde{J};$$

the expression in question is $(T_q - q)(T_q - 1)$.

Discussion of the second theorem

Recall the statement:

Theorem

The annihilator of C in $\mathbf{T}$ is contained in the Eisenstein ideal I.

In the first theorem, we observed that $C \subset J_0(N)$ is small; in fact, we showed that the group of rational torsion points of $J_0(N)$ is small. The second theorem states that C is big in the sense that it has a small annihilator. We prove it by exhibiting a subquotient of C with small annihilator.

At least morally (and quite possibly literally), everything that we need is contained in the work of Kubert–Lang and Stevens.

Discussion of the second theorem

Recall:

- $N \geq 1$, $Y_0(N) \hookrightarrow X_0(N) = Y_0(N) \coprod \{\text{cusps}\}$, all over $\mathbf{Q}$.
- $J_0(N) =$ Jacobian of $X_0(N)$ (Abelian variety over $\mathbf{Q}$).
- $\tilde{C} =$ group of degree-0 divisors on $X_0(N)$ with cuspidal support (formal cuspidal group)
- $C =$ image of $\tilde{C}$ in $J_0(N) =$ cuspidal subgroup of $J_0(N)$.
- Manin–Drinfeld: C is a finite group

Let U be the group of *modular units* on $X_0(N)$, considered modulo scalars. Then $C = \tilde{C}/\operatorname{div}(U)$, where div is the divisor map.

(We continue to tacitly tensor $\mathbf{Z}$-modules with $\mathbf{Z}_{(p)}$ and thus are secretly considering the p-primary part of C.)

Modular units and Eisenstein series

Here's the slogan of the moment:

> *The divisor of a modular unit u is the residue of the differential $\mathrm{dlog}\, u$.*

We complicate things slightly by inserting a middleman. Define the Eisenstein series $\mathcal{D}u$ by the formula

$$2\pi i \mathcal{D}u \, dz = \mathrm{dlog}\, u$$

and introduce the residue map on Eisenstein series

$$\mathrm{Res}\, f = 2\pi i \sum_{c \in \mathrm{cusps}} \mathrm{Res}_c(f(z)\, dz)[c].$$

Then $\mathrm{div}\, u = \mathrm{Res}(\mathcal{D}u)$ for all $u \in U$.

Example

Let d be a divisor of N with $d \neq 1$. A suitable power of the eta-quotient $\eta(dz)/\eta(z)$ is a modular unit on $X_0(N)$. Let $h_d = \left(\frac{\eta(dz)}{\eta(z)}\right)^{12N}$. Then $\mathcal{D}h_d = 12N(e(dz) - e(z))$, where

$$e = -\frac{1}{12} + \sum_{n=1}^{\infty} \big(\sum_{d|N} d \big) q^n$$

is the phantom Eisenstein series of weight 2 on $\mathbf{SL}(2, \mathbf{Z})$. Here, q is the standard variable $2^{2\pi iz}$ and is no longer a prime number.

Note that the q-expansion of this Eisenstein series is $\mathbf{Z}_{(p)}$-integral.

A key proposition

Proposition

If u is a modular unit, then the q-expansion of $\mathcal{D}u$ is $\mathbf{Z}_{(p)}$-integral.

I suspect that this proposition is implicit in the work of Kubert–Lang and Stevens. Our article has a “pure thought” proof using the arithmetic of the arithmetic surface $Y_0(N)_{\mathbf{Z}[\frac{1}{N}]}$.

Some notation

Let $M = M_2(\Gamma_0(N), \mathbf{Z}_{(p)})$ be the space of weight-2 modular forms on $\Gamma_0(N)$ whose q-expansions at ∞ are $\mathbf{Z}_{(p)}$-integral. Let S and E be the submodules of M consisting of cusp forms and Eisenstein series with $\mathbf{Z}_{(p)}$-integral q-expansions. The quotient

$$M/(S \oplus E)$$

is a classic “module of fusion” whose annihilator as a $\mathbf{T}$-module is easily seen to be the Eisenstein ideal I.

We claim that the cuspidal group C has a subquotient isomorphic to $M/(S \oplus E)$. It follows from this claim that the annihilator of C is contained in I, which is precisely the statement of the second theorem.

Proof of the claim

First of all,

$$C = \tilde{C}/\operatorname{div}(U) = \tilde{C}/\operatorname{Res}(\mathcal{D}U) \twoheadrightarrow \tilde{C}/\operatorname{Res}(E),$$

in view of the Proposition. Then the exact sequence

$$0 \to S \to M \xrightarrow{\operatorname{Res}} \tilde{C},$$

makes $M/(S \oplus E)$ into a submodule of $\tilde{C}/\operatorname{Res}(E)$ and therefore a subquotient of $\tilde{C}/\operatorname{Res}(\mathcal{D}U) = C$.

About the cover photo

This photo shows a detail from Mathemalchemy, a mixed-media art installation that resulted from a collaboration between Ingrid Daubechies and Canadian artist Dominique Ehrmann.